General Quantitative Specification Theories with Modalities

Sebastian S. Bauer, Uli Fahrenberg, Axel Legay, Claus Thrane

▶ **To cite this version:**

Sebastian S. Bauer, Uli Fahrenberg, Axel Legay, Claus Thrane. General Quantitative Specification Theories with Modalities. CSR, Jul 2012, Nizhny Novgorod, Russia. pp.18 - 30, 10.1007/978-3-642-30642-6_3 . hal-01087983

HAL Id: hal-01087983

https://inria.hal.science/hal-01087983

Submitted on 27 Nov 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

General Quantitative Specification Theories with Modalities

Sebastian S. Bauer[1], Uli Fahrenberg[2], Axel Legay[2], and Claus Thrane[3]

[1] Ludwig-Maximilians-Universität München, Germany
[2] Irisa/INRIA Rennes, France
[3] Aalborg University, Denmark

Abstract. This paper proposes a new theory of quantitative specifications. It generalizes the notions of step-wise refinement and compositional design operations from the Boolean to an arbitrary quantitative setting. It is shown that this general approach permits to recast many existing problems which arise in system design.

1 Introduction

Specification theories permit reasoning about behaviors of systems at the abstract level, which is needed in various application such as abstraction-based model checking for programming languages, or compositional reasoning. Such specification theories generally come with (1) a satisfaction relation that allows to decide whether an implementation is a model of the specification, (2) a notion of refinement for determining the relationship between specifications and their sets of implementations, (3) a structural composition which, at the abstract level, mimics the behavioral composition of systems, (4) a quotient that allows to synthesize specifications from refinements, and (5) a logical composition that allows to compute intersections of sets of implementations.

Prominent among specification theories is the one of *modal transition systems* [13–15, 18, 21], which are labeled transition systems equipped with two types of transitions: *must* transitions that are mandatory for any implementation, and *may* transitions which are optional. In recent work [3, 17], modal transition systems have been extended by adding richer information to the usual discrete label set of transition systems, permitting to reason about *quantitative* aspects of models and specifications. These quantitative labels can be used to model and analyze *e.g.* timing [6, 16], resource usage [22], or energy consumption [4, 9].

In particular, [17] extends modal transition systems with integer intervals and introduces corresponding extensions of the above operations which observe the added quantitative information, and [3] generalizes this theory to general *structured labels*. Both theories are, however, *fragile* in the sense that they rely on Boolean notions of satisfaction and refinement: as refinement either holds or does not, they are unable to *quantify* the impact of small variations. For quantifying differences, *distances* between systems are useful; this approach has been

explored *e.g.* in [5, 7, 19, 23, 25]. A first quantitative specification theory which is not fragile is introduced in [2], for one specific type of weighted modal transition systems and one specific distance. While this is useful for some applications, it is too specific to cover the whole spectrum of quantitative specification theories.

What is needed is a quantitative specification theory that is independent of both the specific labels and the distance used to measure differences; this is what we introduce in this paper. Using the concept of distance iterator function from [10, 12], we introduce a general notion of refinement distance between structured modal transition systems and a general quantitative specification theory. It turns out that there are some natural technical compatibility conditions relating the label composition operators with the distance which give rise to different properties of the specification theory; these are worked out in detail.

Our general quantitative theory can be instantiated with a variety of different distances and operators, all useful for different applications; hence it can serve as a unifying framework for these applications. Note that all proofs of this paper had to be omitted due to space constraints.

2 Structured Modal Transition Systems

Labeled transition systems have long been established as the de-facto formalism for specifying formal semantics for discrete behavior and communication of programming languages and reactive systems. However, in order to capture meta-data and expectations about these, such as *e.g.* execution times of hardware platforms, cost of certain operations, or energy consumption, we require a richer formalism.

We work with a poset Spec of *specification labels* with a partial order $\sqsubseteq_{\mathsf{Spec}}$ and denote by $\mathsf{Spec}^\infty = \mathsf{Spec}^* \cup \mathsf{Spec}^\omega$ the set of finite and infinite traces over Spec. In applications, Spec may be used to model data about the behavior of a system; for specifications this may be considered as legal parameters of operation, whereas for implementations it may be thought of as observed information. The partial order $\sqsubseteq_{\mathsf{Spec}}$ is meant to model *refinement* of data; if $k \sqsubseteq_{\mathsf{Spec}} \ell$, then k is more refined (leaves fewer choices) than ℓ. The set $\mathsf{Imp} = \{k \in \mathsf{Spec} \mid k' \sqsubseteq_{\mathsf{Spec}} k \implies k' = k\}$ is called the set of *implementation labels*; these are the data which cannot be refined further. We let $[\![k]\!] = \{k' \in \mathsf{Imp} \mid k' \sqsubseteq k\}$ and assume that Spec is well-formed in the sense that $[\![k]\!] \neq \emptyset$ for all $k \in \mathsf{Spec}$.

When $k \not\sqsubseteq_{\mathsf{Spec}} \ell$, we want to be able to quantify the impact of this difference in data on the systems in question, thus circumventing the fragility of the theory. To this end, we introduce a general notion of distance on sequences of data following the approach laid out in [12]. Let M be an arbitrary set and $\mathbb{L} = (\mathbb{R}_{\geq 0} \cup \{\infty\})^M$ the set of functions from M to the extended non-negative real line. Then $\mathbb{L}$ is a complete lattice with partial order $\sqsubseteq_{\mathbb{L}}$ given by $\alpha \sqsubseteq_{\mathbb{L}} \beta$ if and only if $\alpha(x) \leq \beta(x)$ for all $x \in M$, and with an addition $\oplus_{\mathbb{L}}$ given by $(\alpha \oplus_{\mathbb{L}} \beta)(x) = \alpha(x) + \beta(x)$. The bottom element of $\mathbb{L}$ is also the zero of $\oplus_{\mathbb{L}}$ and given by $\bot_{\mathbb{L}}(x) = 0$, and the top element is $\top_{\mathbb{L}}(x) = \infty$. We also define a metric on $\mathbb{L}$ by $d_{\mathbb{L}}(\alpha, \beta) = \sup_{x \in M} |\alpha(x) - \beta(x)|$.

Let $d : \mathsf{Imp} \times \mathsf{Imp} \to \mathbb{L}$ be a hemimetric on implementation labels; recall that this means that $d(m,m) = \bot_{\mathbb{L}}$ for all $m \in \mathsf{Imp}$ and $d(m_1,m_2) \oplus_{\mathbb{L}} d(m_2,m_3) \sqsupseteq_{\mathbb{L}} d(m_1,m_3)$ (the *triangle inequality*) for all $m_1, m_2, m_3 \in \mathsf{Imp}$. We extend d to Spec by $d(k,\ell) = \sup_{m \in [\![k]\!]} \inf_{n \in [\![\ell]\!]} d(m,n)$. Hence also this distance is *asymmetric*; the intuition is that any label in $[\![k]\!]$ has to be matched as good as possible in $[\![\ell]\!]$. Note the similarity of this to the construction of *Hausdorff metric*; *cf.* [20, 1] for background material on hemimetrics and the Hausdorff construction.

We will assume given an abstract *trace distance* $d_T : \mathsf{Spec}^\infty \times \mathsf{Spec}^\infty \to \mathbb{L}$ which has a recursive expression using a *distance iterator* function $F : \mathsf{Imp} \times \mathsf{Imp} \times \mathbb{L} \to \mathbb{L}$. This will allow us to recover many of the system distances found in the literature, while preserving key results. We will need F to be *continuous* in the first two coordinates and *monotone* in the third; hence $F(\cdot, n, \alpha)$ and $F(m, \cdot, \alpha)$ are continuous functions $\mathsf{Imp} \to \mathbb{L}$ for all $\alpha \in \mathbb{L}$,and $F(m,n,\cdot) : \mathbb{L} \to \mathbb{L}$ is monotone for all $m, n \in \mathsf{Imp}$.

We also assume that $F(m,n,\bot_{\mathbb{L}}) = d(m,n)$ for all $m, n \in \mathsf{Imp}$, and we extend F to specification labels by defining $F(k,\ell,\alpha) = \sup_{m \in [\![k]\!]} \inf_{n \in [\![\ell]\!]} F(m,n,\alpha)$. Then also the extended $F : \mathsf{Spec} \times \mathsf{Spec} \times \mathbb{L} \to \mathbb{L}$ is continuous in the first two and monotone in the third coordinates. Additionally, we assume that sets of implementation labels are *closed* with respect to F in the sense that for all $k, \ell \in \mathsf{Spec}$ and $\alpha \in \mathbb{L}$ with $F(k,\ell,\alpha) \neq \top_{\mathbb{L}}$, there are $m \in [\![k]\!]$, $n \in [\![\ell]\!]$ with $F(m,\ell,\alpha) = F(k,n,\alpha) = F(k,\ell,\alpha)$. Note that this implies that the sets $[\![k]\!]$ are closed under the hemimetric d on Spec. We also extend the triangle inequality for d to F by imposing that for all $k, \ell, m \in \mathsf{Spec}$ and $\alpha, \beta, \gamma \in \mathbb{L}$ with $\alpha \oplus_{\mathbb{L}} \beta \sqsupseteq_{\mathbb{L}} \gamma$,

$$F(k,\ell,\alpha) \oplus_{\mathbb{L}} F(\ell,m,\beta) \sqsupseteq_{\mathbb{L}} F(k,m,\gamma). \tag{1}$$

Let $\boldsymbol{\varepsilon} \in \mathsf{Spec}^\infty$ denote the empty sequence, and for any sequence $\sigma \in \mathsf{Spec}^\infty$, denote by σ_0 its first element and by σ^1 the tail of the sequence with the first element removed. We assume that d_T has a recursive characterization, using F, as follows:

$$d_T(\sigma,\tau) = \begin{cases} F(\sigma_0, \tau_0, d_T(\sigma^1, \tau^1)) & \text{if } \sigma, \tau \neq \boldsymbol{\varepsilon}, \\ \top_{\mathbb{L}} & \text{if } \sigma = \boldsymbol{\varepsilon}, \tau \neq \boldsymbol{\varepsilon} \text{ or } \sigma \neq \boldsymbol{\varepsilon}, \tau = \boldsymbol{\varepsilon}, \\ \bot_{\mathbb{L}} & \text{if } \sigma = \tau = \boldsymbol{\varepsilon}. \end{cases} \tag{2}$$

In applications (see below), the lattice $\mathbb{L}$ comes equipped with a homomorphism $g : \mathbb{L} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ for which $g(d_T(\sigma,\sigma)) = 0$ for all $\sigma \in \mathsf{Spec}^\infty$. The actual trace distance of interest is then the composition $g \circ d_T$. The triangle inequality for F implies the usual triangle inequality for $g \circ d_T$: $g(d_T(\sigma,\tau)) + g(d_T(\tau,\chi)) \leq g(d_T(\sigma,\chi))$ for all $\sigma, \tau, \chi \in \mathsf{Spec}^\infty$, hence $g \circ d_T$ is a hemimetric on Spec^∞. We need to work with distances which factor through $\mathbb{L}$, instead of plainly taking values in $\mathbb{R}_{\geq 0} \cup \{\infty\}$, because some distances which are useful in practice, as the one in Example 2 below, have no recursive characterization using $\mathbb{L} = \mathbb{R}_{\geq 0} \cup \{\infty\}$. Whether the theory works for more general intermediate lattices than $L = (\mathbb{R}_{\geq 0} \cup \{\infty\})^M$ is an open question; we have had no occasion to use more general lattices in practice.

Example 1. [2] defines an *accumulating* distance for integer-weighted modal transition systems. In this paper, $\mathsf{Spec} = \Sigma \times \mathbb{I}$, where Σ is a finite set of discrete labels and $\mathbb{I} = \{[l,r] \mid l \in \mathbb{Z} \cup \{-\infty\}, r \in \mathbb{Z} \cup \{\infty\}, l \le r\}$ is the set of extended-integer intervals, and the partial order is defined by $(a,[l,r]) \sqsubseteq_{\mathsf{Spec}} (a',[l',r'])$ if and only if $a = a'$, $l' \le l$, and $r' \ge r$. Hence refinement is given by restricting intervals, thus $\mathsf{Imp} = \Sigma \times \mathbb{Z}$. The implementation label distance is given by $d((a,x),(a',y)) = |x-y|$ if $a = a'$ and ∞ otherwise.

Now let $\mathbb{L} = \mathbb{R}_{\ge 0} \cup \{\infty\}$ and $F(m,n,\alpha) = d(m,n) + \lambda\alpha$ for some fixed *discounting factor* $\lambda \in \mathbb{R}$ with $0 < \lambda < 1$, then $d_T(\sigma,\tau) = \sum_j \lambda^j d(\sigma_j,\tau_j)$ for implementation traces of equal length. This distance hence accumulates individual distances on labels; it has been studied for weighted transition systems and games *e.g.* in [5, 7, 8, 19, 23, 25, 26]. [2] develops a complete specification theory around this specific distance; we will continue this example below to show how it fits in our present context.

Example 2. With the same instantiations of Imp and Spec as above, we can introduce a distance which, instead of accumulating individual label differences, measures the long-run difference between *accumulated labels*. This *maximum-lead* distance is especially useful for real-time systems and has been considered in [16, 23].

Let $\mathbb{L} = (\mathbb{R}_{\ge 0} \cup \{\infty\})^{\mathbb{R}}$, define $F : \mathsf{Imp} \times \mathsf{Imp} \times \mathbb{L} \to \mathbb{L}$ by $F((a,x),(a',y),\alpha) = \top_{\mathbb{L}}$ if $a \ne a'$ and $F((a,x),(a,y),\alpha)(\delta) = \max(|\delta + x - y|, \alpha(\delta + x - y))$, and extend F to specifications by $F(k,\ell,\alpha) = \sup_{m \in [\![k]\!]} \inf_{n \in [\![\ell]\!]} F(m,n,\alpha)$. Define $g : \mathbb{L} \to \mathbb{R}_{\ge 0} \cup \{\infty\}$ by $g(\alpha) = \alpha(0)$; the maximum-lead distance assuming the lead is zero. Using our definition of d_T from (2), it can then be shown that for implementation traces $\sigma = ((a_0,x_0),(a_1,x_1),\dots)$, $\tau = ((a_0,y_0),(a_1,y_1),\dots)$, $g(d_T(\sigma,\tau)) = \sup_m |\sum_{i=0}^m x_i - \sum_{i=0}^m y_i|$ is precisely the maximum-lead distance of [16, 12].

A *structured modal transition system* (SMTS) is a tuple $(S, s_0, \dashrightarrow_S, \longrightarrow_S)$ consisting of a set S of states, an initial state $s_0 \in S$, and *must* and *may* transitions $\longrightarrow_S, \dashrightarrow_S \subseteq S \times \mathsf{Spec} \times S$ for which it holds that for all $s \xrightarrow{k}_S s'$ there is $s \overset{\ell}{\dashrightarrow}_S s'$ with $k \sqsubseteq_{\mathsf{Spec}} \ell$. This last condition is one of *consistency*: everything which is required, is also allowed. S is an *implementation* if $\longrightarrow_S = \dashrightarrow_S \subseteq S \times \mathsf{Imp} \times S$; hence in an implementation, all optional behavior has been resolved, and all data has been refined to implementation labels.

We will assume all SMTS to be *compactly branching* [24], that is, for any SMTS S and any $s \in S$, the sets $\{k \in \mathsf{Spec} \mid s \overset{k}{\dashrightarrow} s'\}$ and $\{k \in \mathsf{Spec} \mid s \xrightarrow{k} s'\}$ are to be compact under the label metric d. This is a common assumption in quantitative formalisms which generalizes the standard finitely-branching assumption; together with continuity of F it will allow us to resolve terms of the form $\sup_{s \overset{k}{\dashrightarrow} s'} \inf_{t \overset{\ell}{\dashrightarrow} t'} F(k,\ell,\alpha)$.

The SMTS $(S, s_0, \dashrightarrow_S, \longrightarrow_S)$ is *deterministic* if it holds for all $s \in S$, $s \overset{k_1}{\dashrightarrow}_S s_1$, $s \overset{k_2}{\dashrightarrow}_S s_2$ for which there is $k \in \mathsf{Spec}$ with $d(k,k_1) \ne \top_{\mathbb{L}}$ and $d(k,k_2) \ne \top_{\mathbb{L}}$ that $k_1 = k_2$ and $s_1 = s_2$.

Example 1 (contd). For the label distance of [2], and also the one of Example 2, the above condition that there exist $k \in \mathsf{Spec}$ with $d(k, k_1) \neq \top_{\mathbb{L}}$ and $d(k, k_2) \neq \top_{\mathbb{L}}$ is equivalent, with $k_1 = (a_1, I_1)$ and $k_2 = (a_2, I_2)$, to saying that $a_1 = a_2$, hence our notion of determinism agrees with the one of [2]. The general intuition for determinacy is that there cannot be two distinct transitions out of a state with labels which have a common quantitative refinement.

A *modal refinement* of SMTS S, T is a relation $R \subseteq S \times T$ such that for any $(s, t) \in R$,

- whenever $s \overset{k}{\dashrightarrow}_S s'$, then also $t \overset{\ell}{\dashrightarrow}_T t'$ for some $k \sqsubseteq_{\mathsf{Spec}} \ell$ and $(s', t') \in R$,
- whenever $t \overset{\ell}{\longrightarrow}_T t'$, then also $s \overset{k}{\longrightarrow}_S s'$ for some $k \sqsubseteq_{\mathsf{Spec}} \ell$ and $(s', t') \in R$.

Thus any behavior which is permitted in S is also permitted in T, and any behavior required in T is also required in S. We write $S \leq_m T$ if there is a modal refinement $R \subseteq S \times T$ with $(s_0, t_0) \in R$. The *implementation semantics* of a SMTS S is the set $[\![S]\!] = \{I \leq_m S \mid I \text{ is an implementation}\}$, and we write $S \leq_t T$ if $[\![S]\!] \subseteq [\![T]\!]$, saying that S thoroughly refines T.

3 Refinement Distances

We define two distances between SMTS, one at the syntactic and one at the semantic level. The *modal refinement distance* $d_m : S \times T \to \mathbb{L}$ between the states of SMTS S, T is defined to be the least fixed point to the equations

$$d_m(s,t) = \max \begin{cases} \sup\limits_{s \overset{k}{\dashrightarrow}_S s'} \inf\limits_{t \overset{\ell}{\dashrightarrow}_T t'} F(k, \ell, d_m(s', t')), \\ \sup\limits_{t \overset{\ell}{\longrightarrow}_T t'} \inf\limits_{s \overset{k}{\longrightarrow}_S s'} F(k, \ell, d_m(s', t')). \end{cases}$$

We let $d_m(S, T) = d_m(s_0, t_0)$, and we write $S \leq_m^{\alpha} T$ if $d_m(S, T) \sqsubseteq_{\mathbb{L}} \alpha$. This definition is an extension of the one of *simulation distance* in [12], and the proof of existence of the least fixed point is similar to the one in [12]. Note also that d_m extends the refinement relation $\leq_m$ in the sense that $s \leq_m t$ implies $d_m(s, t) = 0$. If we define the *linear distance* from s to t by $d_T(s, t) = \max\{\sup_{\sigma \in \mathrm{Tr}(s)} \inf_{\tau \in \mathrm{Tr}(t)} d_T(\sigma, \tau), \sup_{\tau \in \mathrm{Tr}(t)} \inf_{\sigma \in \mathrm{Tr}(s)} d_T(\sigma, \tau)\}$, where $\mathrm{Tr}(s)$ denotes the set of (*may* or *must*) traces emanating from s, then $d_T(s, t) \sqsubseteq_{\mathbb{L}} d_m(s, t)$ for all $s, t \in S$, *cf.* [12].

The *thorough refinement distance* from an SMTS S to an SMTS T is

$$d_t(S, T) = \sup_{I \in [\![S]\!]} \inf_{J \in [\![T]\!]} d_m(I, J),$$

and we write $S \leq_t^{\alpha} T$ if $d_t(S, T) \sqsubseteq_{\mathbb{L}} \alpha$. Again, $S \leq_t T$ implies $d_t(S, T) = 0$. The next proposition follows directly from the triangle inequality (1).

Proposition 1. *For all SMTS S, T, U, $d_m(S, T) \oplus_{\mathbb{L}} d_m(T, U) \sqsupseteq_{\mathbb{L}} d_m(S, U)$ and $d_t(S, T) \oplus_{\mathbb{L}} d_t(T, U) \sqsupseteq_{\mathbb{L}} d_t(S, U)$.*

The next theorem shows that the modal refinement distance overapproximates the thorough one, and that it is exact for deterministic SMTS. This is similar to the situation for standard modal transition systems [18]; note [18] that deterministic specifications generally suffice for applications.

Theorem 1. *For all SMTS S, T, $d_t(S,T) \sqsubseteq_{\mathbb{L}} d_m(S,T)$. If T is deterministic, then $d_t(S,T) = d_m(S,T)$.*

In a quantitative framework, it can be useful to be able to *relax* and *strengthen* specifications during the development process. Which precise relaxations and strengthenings one wishes to apply will depend on the actual application, but we can here show three general relaxations which differ from each other in the *level* of the theory at which they are applied. For $\alpha \in \mathbb{L}$ and SMTS S, T,

- T is an *α-widening* of S if there is a relation $R \subseteq S \times T$ for which $(s_0, t_0) \in R$ and such that for all $(s,t) \in R$, $s \overset{k}{\dashrightarrow}_S s'$ if and only if $t \overset{\ell}{\dashrightarrow}_T t'$, and $s \overset{k}{\longrightarrow}_S s'$ if and only if $t \overset{\ell}{\longrightarrow}_T t'$, for $k \sqsubseteq_{\mathsf{Spec}} \ell$, $d(\ell, k) \sqsubseteq_{\mathbb{L}} \alpha$, and $(s', t') \in R$;
- T is an *α-relaxation* of S if $S \leq_m T$ and $T \leq_m^\alpha S$;
- the *α-extended implementation semantics* of S is $[\![S]\!]^{+\alpha} = \{I \leq_m^\alpha S \mid I \text{ implementation}\}$.

Hence α-widening is an entirely *syntactic* notion: up to unweighted bisimulation, T is the same as S, but transition labels in T can be α "wider" than in S (hence also $S \leq_m T$). The second notion, α-relaxation, works at the level of semantics of specifications, whereas the last notion is at implementation level. A priori, there is no relation between the syntactic and semantic notions, even though one can be established in some special cases.

Example 1 (contd). In [2] it is shown that for the accumulated distance with discounting factor λ, any α-widening is also a $(1-\lambda)^{-1}\alpha$-relaxation. This is due to the fact that for traces $\sigma, \tau \in \mathsf{Spec}^\infty$ with $d(\sigma_j, \tau_j) \leq \alpha$ for all j, we have $\sum_j \lambda^j d(\sigma_j, \tau_j) \leq \sum_j \lambda^j \alpha \leq (1-\lambda)^{-1}\alpha$ by convergence of the geometric series.

Example 2 (contd). For the maximum-lead distance, it is easy to expose cases of α-widenings which are not β-relaxations for any β. One example consists of two one-state SMTS S, T with loops $s_0 \overset{a,1}{\longrightarrow} s_0$ and $t_0 \overset{a,[0,2]}{\longrightarrow} t_0$; then T is a 1-widening of S, but $g \circ d_m(T,S) = \infty$.

Proposition 2. *If T is an α-relaxation of S, then $[\![T]\!] \subseteq [\![S]\!]^{+\alpha}$.*

It can be shown for special cases that the inclusion in the proposition is strict [2]; for the proof one only needs the fact that $d_m(I,S) \sqsubseteq d_m(I,T) \oplus d_m(T,S) \sqsubseteq_{\mathbb{L}} \alpha$ for all $I \in [\![T]\!]$.

Proposition 3. *Let T be an α-relaxation of S and T' an α'-relaxation of S', and let $d_m(S,S') = \beta$. Then $\beta \sqsubseteq_{\mathbb{L}} d_m(S,T') \oplus_{\mathbb{L}} \alpha'$, $d_m(S,T') \sqsubseteq \beta$, $\beta \sqsubseteq_{\mathbb{L}} d_m(T,S')$, and $d_m(T,S') \oplus_{\mathbb{L}} \alpha \sqsubseteq_{\mathbb{L}} \beta$.*

4 Structural Composition and Quotient

We now introduce the different operations on SMTS which make up a specification theory. Firstly, we are interested in composing specifications S, S' into a specification $S\|S'$ by synchronizing on shared actions and with interleaving for non-shared actions. Secondly, we need a quotient operator which solves equations of the form $S\|X \equiv T$, that is, the quotient synthesizes the most general specification $T \oslash S$ which describes all SMTS X satisfying the above equation. We first define a partial *label synchronization* operator $\oplus : \mathsf{Spec} \times \mathsf{Spec} \hookrightarrow \mathsf{Spec}$ which satisfies the following conditions:

- For all $k, \ell, k', \ell' \in \mathsf{Spec}$, if $d(k,\ell) \neq \top_{\mathbb{L}}$ and $d(k',\ell') \neq \top_{\mathbb{L}}$, then $k \oplus k'$ is defined if and only if $\ell \oplus \ell'$ is defined;
- for all $\ell, \ell' \in \mathsf{Spec}$, $(\exists k \in \mathsf{Spec} : d(k,\ell) \neq \top_{\mathbb{L}}, d(k,\ell') \neq \top_{\mathbb{L}}) \iff (\exists m \in \mathsf{Spec} : \ell \oplus m, \ell' \oplus m$ are defined).

This operator permits to synchronize labels at transitions which are executed in parallel; the first property ensures that refinements of synchronable labels can synchronize and *vice versa*, and the second relates synchronizability to distances in such a way that two labels have a common quantitative refinement if and only if they have a common synchronization.

Additionally, we must assume that there exists a function $P : \mathbb{L} \times \mathbb{L} \to \mathbb{L}$ which allows us to infer bounds on distances on synchronized labels. We assume that P is monotone in both coordinates, has $P(\bot_{\mathbb{L}}, \bot_{\mathbb{L}}) = \bot_{\mathbb{L}}$, $P(\alpha, \top_{\mathbb{L}}) = P(\top_{\mathbb{L}}, \alpha) = \top_{\mathbb{L}}$ for all $\alpha \in \mathbb{L}$, and that

$$F(k \oplus k', \ell \oplus \ell', P(\alpha,\alpha')) \sqsubseteq_{\mathbb{L}} P(F(k,\ell,\alpha), F(k',\ell',\alpha'))$$

for all $k, \ell, k', \ell' \in \mathsf{Spec}$ and $\alpha, \alpha' \in \mathbb{L}$ for which $k \oplus k'$ and $\ell \oplus \ell'$ are defined. Hence $d(k \oplus k', \ell \oplus \ell') \sqsubseteq_{\mathbb{L}} P(d(k,\ell), d(k',\ell'))$ for all such $k, \ell, k', \ell' \in \mathsf{Spec}$, thus P indeed bounds distances of synchronized labels.

The *structural composition* of two SMTS S and T is the SMTS $S\|T = (S \times T, (s_0,t_0), \dashrightarrow_{S\|T}, \longrightarrow_{S\|T})$ with transitions defined as follows:

$$\frac{s \overset{k}{\dashrightarrow}_S s' \quad t \overset{\ell}{\dashrightarrow}_T t' \quad k \oplus \ell \text{ defined}}{(s,t) \overset{k\oplus\ell}{\dashrightarrow}_{S\|T} (s',t')} \qquad \frac{s \overset{k}{\longrightarrow}_S s' \quad t \overset{\ell}{\longrightarrow}_T t' \quad k \oplus \ell \text{ defined}}{(s,t) \overset{k\oplus\ell}{\longrightarrow}_{S\|T} (s',t')}$$

The next theorem shows that structural composition supports *independent implementability*: if S is close to T and S' close to T', then we can bound the distance between the structural compositions.

Theorem 2. *For SMTS S, T, S', T', $d_m(S\|S', T\|T') \sqsubseteq_{\mathbb{L}} P(d_m(S,T), d_m(S',T'))$.*

Example 1 (contd). In [2], structural composition of labels is defined by

$$(a,[l,r]) \oplus (a',[l',r']) = \begin{cases} (a,[l+l', r+r']) & \text{if } a = a', \\ \text{undefined} & \text{otherwise.} \end{cases}$$

This composition is bounded above by $P(\alpha,\alpha') = \alpha + \alpha'$, hence Theorem 2 specializes to [2, Thm. 5]: $d_m(S\|S', T\|T') \leq d_m(S,T) + d_m(S',T')$.

Example 2 (contd). For the max-lead distance, and with an application to real-time systems in mind, structural composition is more naturally defined using *intersection* of intervals rather than addition, that is,

$$(a,[l,r]) \oslash (a',[l',r']) = \begin{cases} (a,[\max(l,l'),\min(r,r')]) & \\ \qquad\qquad & \text{if } a=a' \text{ and } \max(l,l') \le \min(r,r'), \\ \text{undefined} & \text{otherwise.} \end{cases}$$

(Note that, however, the definition of structural composition is independent of which distance one uses; one might as well combine addition of intervals, as in Example 1, with the max-lead distance.) This composition is bounded by $P(\alpha,\alpha') = \max(\alpha,\alpha')$, thus $d_m(S\|S',T\|T') \le \max(d_m(S,T)+d_m(S',T'))$.

For *quotients* of SMTS, we need a partial label operator $\oslash : \mathsf{Spec} \times \mathsf{Spec} \to \mathsf{Spec}$ for which it holds that

- for all $k,\ell,m \in \mathsf{Spec}$, $\ell \oslash k$ is defined and $m \sqsubseteq_{\mathsf{Spec}} \ell \oslash k$ if and only if $k \oslash m$ is defined and $k \oslash m \sqsubseteq_{\mathsf{Spec}} \ell$;
- for all $\ell,\ell' \in \mathsf{Spec}$, $(\exists k \in \mathsf{Spec} : d(k,\ell) \neq \top_{\mathbb{L}}, d(k,\ell') \neq \top_{\mathbb{L}}) \iff (\exists m \in \mathsf{Spec} : m \oslash \ell, m \oslash \ell'$ are defined).

The first condition ensures that $\oslash$ is inverse to $\oslash$, and the second relates it to distances just as we did for $\oslash$ above. We extend the first condition to say that $\oslash$ is *quantitatively well-behaved* if it holds for all $k,\ell,m \in \mathsf{Spec}$ that $\ell \oslash k$ is defined and $d(m,\ell \oslash k) \neq \top_{\mathbb{L}}$ if and only if $k \oslash m$ is defined and $d(k \oslash m,\ell) \neq \top_{\mathbb{L}}$, and in that case, $F(m,\ell \oslash k,\alpha) \sqsupseteq_{\mathbb{L}} F(k \oslash m,\ell,\alpha)$ for all $\alpha \in \mathbb{L}$. We say that $\oslash$ is *quantitatively exact* if the inequality can be sharpened to $F(m,\ell \oslash k,\alpha) = F(k \oslash m,\ell,\alpha)$.

In the definition of quotient below, we denote by $\rho_B(S)$ the *pruning* of a SMTS S with respect to the states in $B \subseteq S$, which is obtained as follows. Define a *must*-predecessor operator $\mathsf{pre} : 2^S \to 2^S$ by $\mathsf{pre}(S') = \{s \in S \mid \exists k \in \mathsf{Spec}, s' \in S' : s \xrightarrow{k} s'\}$ and let pre^* be the reflexive, transitive closure of pre. Then $\rho_B(S)$ exists if $s_0 \notin \mathsf{pre}^*(B)$, and in that case, $\rho_B(S) = (S_\rho, s_0, \dashrightarrow_\rho, \longrightarrow_\rho)$ with $S_\rho = S \setminus \mathsf{pre}^*(B)$, $\dashrightarrow_\rho = \dashrightarrow \cap (S_\rho \times \mathsf{Spec} \times S_\rho)$, and $\longrightarrow_\rho = \longrightarrow \cap (S_\rho \times \mathsf{Spec} \times S_\rho)$.

For SMTS S, T, the *quotient* of T by S is the SMTS $T \setminus\!\!\setminus S = \rho_B(T \times S \cup \{u\}, (t_0,s_0), \dashrightarrow_{T\setminus\!\!\setminus S}, \longrightarrow_{T\setminus\!\!\setminus S})$ given as follows (if it exists):

$$\frac{t \overset{\ell}{\dashrightarrow}_T t' \quad s \overset{k}{\dashrightarrow}_S s' \quad \ell \oslash k \text{ defined}}{(t,s) \overset{\ell\oslash k}{\dashrightarrow}_{T\setminus\!\!\setminus S} (t',s')} \qquad \frac{t \overset{\ell}{\longrightarrow}_T t' \quad s \overset{k}{\longrightarrow}_S s' \quad \ell \oslash k \text{ defined}}{(t,s) \overset{\ell\oslash k}{\longrightarrow}_{T\setminus\!\!\setminus S} (t',s')}$$

$$\frac{t \overset{\ell}{\longrightarrow}_T t' \quad \forall s \overset{k}{\longrightarrow}_S s' : \ell \oslash k \text{ undefined}}{(t,s) \in B}$$

$$\frac{m \in \mathsf{Spec} \quad \forall s \overset{k}{\dashrightarrow}_S s' : k \oslash m \text{ undefined}}{(t,s) \overset{m}{\dashrightarrow}_{T\setminus\!\!\setminus S} u} \qquad \frac{m \in \mathsf{Spec}}{u \overset{m}{\dashrightarrow}_{T\setminus\!\!\setminus S} u}$$

The next theorem shows that under certain standard conditions, quotient is *sound* and *maximal* with respect to $\|$. Note that the property that $X \le_m T \setminus\!\!\setminus S$

iff $S \| X \leq_m T$ implies *uniqueness* of quotient [11]; hence if a certain instantiation of our framework admits a quotient which is not quantitatively well-behaved, there is no hope that one can find another one which is.

Theorem 3. *Let S, T, X be SMTS such that S is deterministic and $T \setminus\!\setminus S$ exists. Then $X \leq_m T \setminus\!\setminus S$ if and only if $S \| X \leq_m T$. Also,*

- *if $\oslash$ is quantitatively well-behaved, then $d_m(X, T \setminus\!\setminus S) \sqsupseteq_{\mathbb{L}} d_m(S \| X, T)$;*
- *if $\oslash$ is quantitatively exact and $d_m(X, T \setminus\!\setminus S) \neq \top_{\mathbb{L}}$, then $d_m(X, T \setminus\!\setminus S) = d_m(S \| X, T)$.*

Example 1 (contd). In [2], quotient of labels is defined by

$$(a', [l', r']) \oslash (a, [l, r]) = \begin{cases} (a, [l' - l, r' - r]) & \text{if } a = a' \text{ and } l' - l \leq r' - r, \\ \text{undefined} & \text{otherwise.} \end{cases}$$

This operator is quantitatively exact, hence Theorem 3 specializes to [2, Thm. 6]: if $d_m(X, T \setminus\!\setminus S) \neq \infty$, then $d_m(X, T \setminus\!\setminus S) = d_m(S \| X, T)$.

Example 2 (contd). For structural composition using interval intersection, it can be shown that $\oslash$ given by

$$(a', [l', r']) \oslash (a, [l, r]) = \begin{cases} \text{undefined} & \text{if } a \neq a', \\ (a, [l', \infty]) & \text{if } a = a' \text{ and } l < l' \leq r \leq r', \\ (a, [l', r']) & \text{if } a = a' \text{ and } l < l' \leq r' < r, \\ \text{undefined} & \text{if } a = a' \text{ and } l \leq r < l' \leq r', \\ (a, [-\infty, \infty]) & \text{if } a = a' \text{ and } l' \leq l \leq r \leq r', \\ (a, [-\infty, r']) & \text{if } a = a' \text{ and } l' \leq l \leq r < r', \\ \text{undefined} & \text{if } a = a' \text{ and } l' \leq r' < l \leq r. \end{cases}$$

yields a quotient operator which is quantitatively well-behaved, but *not* exact. Theorem 3 implies that $d_m(X, T \setminus\!\setminus S) \geq d_m(S \| X, T)$ if if $d_m(X, T \setminus\!\setminus S) \neq \infty$.

5 Conjunction

Conjunction of SMTS can be used to merge two specifications into one. Let $\owedge : \mathsf{Spec} \times \mathsf{Spec} \to \mathsf{Spec}$ be a partial label operator for which it holds that

- for all $k, \ell \in \mathsf{Spec}$, if $k \owedge \ell$ is defined, then $k \owedge \ell \sqsubseteq_{\mathsf{Spec}} k$, $k \owedge \ell \sqsubseteq_{\mathsf{Spec}} \ell$, and
- for all $\ell, \ell' \in \mathsf{Spec}$, $(\exists k \in \mathsf{Spec} : d(k, \ell) \neq \top_{\mathbb{L}}, d(k, \ell') \neq \top_{\mathbb{L}}) \iff (\exists m \in \mathsf{Spec} : \ell \owedge m, \ell' \owedge m$ are defined).

The first requirement above ensures that conjunction acts as a lower bound, and the second one relates it to distances such that two labels have a common refinement if and only if they have a common conjunction. One also usually wants conjunction to be a *greatest* lower bound; we say that $\owedge$ is *conjunctively compositional* if it holds for all $k, \ell, m \in \mathsf{Spec}$ for which $m \sqsubseteq_{\mathsf{Spec}} k$ and $m \sqsubseteq_{\mathsf{Spec}} \ell$ that also $k \owedge \ell$ is defined and $m \sqsubseteq_{\mathsf{Spec}} k \owedge \ell$.

As a quantitative generalization, and analogously to what we did for structural composition, we say that $\otimes$ is *conjunctively bounded* by a function $C : \mathbb{L} \times \mathbb{L} \to \mathbb{L}$ if C is monotone in both coordinates, has $C(\bot_\mathbb{L}, \bot_\mathbb{L}) = \bot_\mathbb{L}$, $C(\alpha, \top_\mathbb{L}) = C(\top_\mathbb{L}, \alpha) = \top_\mathbb{L}$ for all $\alpha \in \mathbb{L}$, and if it holds for all $k, \ell, m \in \mathsf{Spec}$ for which $d(m,k) \neq \top_\mathbb{L}$ and $d(m,\ell) \neq \top_\mathbb{L}$ that $k \otimes \ell$ is defined and

$$F(m, k \otimes \ell, C(\alpha, \alpha')) \sqsubseteq_\mathbb{L} C(F(m,k,\alpha), F(m,\ell,\alpha'))$$

for all $\alpha, \alpha' \in \mathbb{L}$. Note that this implies that $d(m, k \otimes \ell) \sqsubseteq_\mathbb{L} C(d(m,k), d(m,\ell))$, hence conjunctive boundedness implies conjunctive compositionality.

The *conjunction* of two SMTS S and T is the SMTS $S \wedge T = \rho_B(S \times T, (s_0, t_0), \dashrightarrow_{S\wedge T}, \longrightarrow_{S\wedge T})$ given as follows:

$$\frac{s \xrightarrow{k}_S s' \quad t \overset{\ell}{\dashrightarrow}_T t' \quad k \otimes \ell \text{ defined}}{(s,t) \xrightarrow{k\otimes\ell}_{S\wedge T} (s',t')} \qquad \frac{s \overset{k}{\dashrightarrow}_S s' \quad t \xrightarrow{\ell}_T t' \quad k \otimes \ell \text{ defined}}{(s,t) \xrightarrow{k\otimes\ell}_{S\wedge T} (s',t')}$$

$$\frac{s \overset{k}{\dashrightarrow}_S s' \quad t \overset{\ell}{\dashrightarrow}_T t' \quad k \otimes \ell \text{ defined}}{(s,t) \overset{k\otimes\ell}{\dashrightarrow}_{S\wedge T} (s',t')}$$

$$\frac{s \xrightarrow{k}_S s' \quad \forall t \overset{\ell}{\dashrightarrow}_T t' : k \otimes \ell \text{ undef.}}{(s,t) \in B} \qquad \frac{t \xrightarrow{\ell}_T t' \quad \forall s \overset{k}{\dashrightarrow}_S s' : k \otimes \ell \text{ undef.}}{(s,t) \in B}$$

The next theorem shows the precise conditions under which conjunction is a greatest lower bound. Note that the greatest-lower-bound condition $U \leq_m S$, $U \leq_m T \implies U \leq_m S \wedge T$ entails uniqueness.

Theorem 4. *Let S, T, U be SMTS. If $S \wedge T$ is defined, then $S \wedge T \leq_m S$ and $S \wedge T \leq_m T$. If, additionally, S or T are deterministic, then:*

- *If $\otimes$ is conjunctively compositional, $U \leq_m S$, and $U \leq_m T$, then $S \wedge T$ is defined and $U \leq_m S \wedge T$.*
- *If $\otimes$ is conjunctively bounded by C, $d_m(U,S) \neq \top_\mathbb{L}$, and $d_m(U,T) \neq \top_\mathbb{L}$, then $S \wedge T$ is defined and $d_m(U, S \wedge T) \sqsubseteq_\mathbb{L} C(d_m(U,S), d_m(U,T))$.*

Example 1 (contd). For the formalism of [2], there is a conjunction operator $\otimes$ given by intersection of intervals:

$$(a,[l,r]) \otimes (a',[l',r']) = \begin{cases} (a, [\max(l,l'), \min(r,r')]) & \text{if } a = a', \max(l,l') \leq \min(r,r'), \\ \text{undefined} & \text{otherwise.} \end{cases}$$

This operator is conjunctively compositional, but not conjunctively bounded, whence [2, Thm. 4]: by uniqueness, there does not exist any bounded conjunction operator within the formalism of [2].

To deal with the problem that, as in Example 1, conjunction may not be conjunctively bounded, we introduce another, weaker, property which ensures some compatibility of conjunction with distances. We say that $\otimes$ is *relaxed conjunctively bounded* by a function family $C = \{C_{\beta,\gamma} : \mathbb{L} \times \mathbb{L} \to \mathbb{L} \mid \beta, \gamma \in \mathbb{L}\}$ if all $C_{\beta,\gamma}$ are monotone in both coordinates, have $C_{\beta,\gamma}(\bot_\mathbb{L}, \bot_\mathbb{L}) = \bot_\mathbb{L}$, $C_{\beta,\gamma}(\alpha, \top_\mathbb{L}) =$

$C_{\beta,\gamma}(\top_{\mathbb{L}}, \alpha) = \top_{\mathbb{L}}$ for all $\alpha \in \mathbb{L}$, and if it holds for all $k, \ell \in \mathsf{Spec}$ for which there is $m \in \mathsf{Spec}$ with $d(m,k) \neq \top_{\mathbb{L}}$ and $d(m,\ell) \neq \top_{\mathbb{L}}$ that there exist $k', \ell' \in \mathsf{Spec}$ with $k \sqsubseteq_{\mathsf{Spec}} k'$, $\ell \sqsubseteq_{\mathsf{Spec}} \ell'$, $d(k',k) = \beta \neq \top_{\mathbb{L}}$, and $d(\ell',\ell) = \gamma \neq \top_{\mathbb{L}}$, such that $k' \oslash \ell'$ is defined, and then for all $m \in \mathsf{Spec}$ with $d(m,k) \neq \top_{\mathbb{L}}$ and $d(m,\ell) \neq \top_{\mathbb{L}}$,

$$F(m, k' \oslash \ell', C_{\beta,\gamma}(\alpha,\alpha')) \sqsubseteq_{\mathbb{L}} C_{\beta,\gamma}(F(m,k,\alpha), F(m,\ell,\alpha'))$$

for all $\alpha, \alpha' \in \mathbb{L}$. The following theorem shows that relaxed boundedness of $\oslash$ entails a similar property for conjunction.

Theorem 5. *Let S, T be SMTS with S or T deterministic and $\oslash$ relaxed conjunctively bounded by C. If there is an SMTS U for which $d_m(U,S), d_m(U,T) \neq \top_{\mathbb{L}}$, then there exist β- and γ-widenings S' of S and T' of T for which $S' \wedge T'$ is defined, and such that $d_m(U, S' \wedge T') \sqsubseteq_{\mathbb{L}} C_{\beta,\gamma}(d_m(U,S), d_m(U,T))$ for all SMTS U for which $d_m(U,S) \neq \top_{\mathbb{L}}$ and $d_m(U,T) \neq \top_{\mathbb{L}}$.*

Example 1 (contd). For the accumulating distance, $\oslash$ is relaxed conjunctively bounded by $C_{\beta,\gamma}(\alpha,\alpha') = \max(\alpha,\alpha') \oplus_{\mathbb{L}} \max(\beta,\gamma)$. Hence Theorem 5 entails that if S or T are deterministic and there is U for which $d_m(U,S), d_m(U,T) \neq \infty$, then there exist a β-widening S' of S and a γ-widening T' of T for which the conjunction $S' \wedge T'$ is defined, and such that $d_m(U, S' \wedge T') \leq \max(d_m(U,S), d_m(U,T)) + \max(\beta,\gamma)$ for all SMTS U for which $d_m(U,S) \neq \top_{\mathbb{L}}$ and $d_m(U,T) \neq \top_{\mathbb{L}}$.

Example 2 (contd). Also for the max-lead distance, $\oslash$ given by intersection of intervals is the unique conjunction operator. It is again relaxed conjunctively bounded by $C_{\beta,\gamma}(\alpha,\alpha') = \max(\alpha,\alpha') \oplus_{\mathbb{L}} \max(\beta,\gamma)$, hence the same specialization of Theorem 5 as above holds for the max-lead distance.

6 Conclusion

We believe that this paper constitutes the first general and complete quantitative theory for modal specifications. We have shown not only how to introduce such a general quantitative framework, but also the general conditions one needs to impose on the interplay between the system distance and the operators such as composition and quotient for the quantitative theory to work properly.

Using [2] and our running example of max-lead distances, we have seen two different instantiations of the general framework, using different distances for measuring variations of systems and specifications and different operators for structural composition and quotient. Application of our framework *e.g.* to real-time and hybrid systems, in programming languages or quantitative logics, will require other distances and other operators, but as shown in [10, 12], they all stay within the unifying framework introduced in this paper.

References

1. C. D. Aliprantis and K. C. Border. *Infinite Dimensional Analysis: A Hitchhiker's Guide*. Springer, 2007.

2. S. S. Bauer, U. Fahrenberg, L. Juhl, K. G. Larsen, A. Legay, and C. Thrane. Quantitative refinement for weighted modal transition systems. In *MFCS*, vol. 6907 of *LNCS*, pp. 60–71. Springer, 2011.
3. S. S. Bauer, L. Juhl, K. G. Larsen, A. Legay, and J. Srba. Extending modal transition systems with structured labels. *Math. Struct. CS*, 2011. To appear.
4. P. Bouyer, U. Fahrenberg, K. G. Larsen, and N. Markey. Quantitative analysis of real-time systems using priced timed automata. *CACM*, 54(9):78–87, 2011.
5. K. Chatterjee, L. Doyen, and T. A. Henzinger. Quantitative languages. *ACM Trans. Comp. Logic*, 11(4), 2010.
6. A. David, K. G. Larsen, A. Legay, U. Nyman, and A. Wąsowski. Timed I/O automata: A complete specification theory for real-time systems. In *HSCC*, pp. 91–100. ACM, 2010.
7. L. de Alfaro, M. Faella, and M. Stoelinga. Linear and branching system metrics. *IEEE Trans. Soft. Eng.*, 35(2):258–273, 2009.
8. A. Ehrenfeucht and J. Mycielski. Positional strategies for mean payoff games. *Int. J. Game Th.*, 8:109–113, 1979.
9. U. Fahrenberg, L. Juhl, K. G. Larsen, and J. Srba. Energy games in multiweighted automata. In *ICTAC*, vol. 6916 of *LNCS*, pp. 95–115. Springer, 2011.
10. U. Fahrenberg, A. Legay, and C. Thrane. The quantitative linear-time–branching-time spectrum. In *FSTTCS*, vol. 13 of *LIPIcs*, pp. 103–114, 2011.
11. U. Fahrenberg, A. Legay, and A. Wąsowski. Make a difference! (Semantically). In *MoDELS*, vol. 6981 of *LNCS*, pp. 490–500. Springer, 2011.
12. U. Fahrenberg, C. Thrane, and K. G. Larsen. Distances for weighted transition systems: Games and properties. In *QAPL*, vol. 57 of *EPTCS*, pp. 134–147, 2011.
13. P. Godefroid, M. Huth, and R. Jagadeesan. Abstraction-based model checking using modal transition systems. In *CONCUR*, vol. 2154 of *LNCS*. Springer, 2001.
14. A. Gruler, M. Leucker, and K. D. Scheidemann. Modeling and model checking software product lines. In *FMOODS*, vol. 5051 of *LNCS*. Springer, 2008.
15. O. Grumberg, M. Lange, M. Leucker, and S. Shoham. Don't know in the μ-calculus. In *VMCAI*, vol. 3385 of *LNCS*, pp. 233–249. Springer, 2005.
16. T. A. Henzinger, R. Majumdar, and V. S. Prabhu. Quantifying similarities between timed systems. In *FORMATS*, vol. 3829 of *LNCS*, pp. 226–241. Springer, 2005.
17. L. Juhl, K. G. Larsen, and J. Srba. Modal transition systems with weight intervals. *J. Logic Alg. Prog.*, 2011. To appear.
18. K. G. Larsen. Modal specifications. In *Automatic Verification Methods for Finite State Systems*, vol. 407 of *LNCS*, pp. 232–246. Springer, 1989.
19. K. G. Larsen, U. Fahrenberg, and C. Thrane. Metrics for weighted transition systems: Axiomatization and complexity. *Th. Comp. Sci.*, 412(28):3358–3369, 2011.
20. J. R. Munkres. *Topology*. Prentice Hall, 2000.
21. U. Nyman. *Modal Transition Systems as the Basis for Interface Theories and Product Lines*. PhD thesis, Aalborg University, September 2008.
22. J. I. Rasmussen, K. G. Larsen, and K. Subramani. On using priced timed automata to achieve optimal scheduling. *Formal Meth. Syst. Design*, 29(1):97–114, 2006.
23. C. Thrane, U. Fahrenberg, and K. G. Larsen. Quantitative simulations of weighted transition systems. *J. Logic Alg. Prog.*, 79(7):689–703, 2010.
24. F. van Breugel. A theory of metric labelled transition systems. *Annals of the New York Academy of Sciences*, 806(1):69–87, 1996.
25. F. van Breugel. A behavioural pseudometric for metric labelled transition systems. In *CONCUR*, vol. 3653 of *LNCS*, pp. 141–155. Springer, 2005.
26. U. Zwick and M. Paterson. The complexity of mean payoff games. In *Computing and Combinatorics*, vol. 959 of *LNCS*, pp. 1–10. Springer, 1995.

Appendix: Proofs

Before we attempt the proofs of the theorems in the paper, we introduce a powerful proof technique which will be used throughout: A *modal refinement family* from S to T, for SMTS S, T, is an $\mathbb{L}$-indexed family of relations $R = \{R_\alpha \subseteq S \times T \mid \alpha \in \mathbb{L}\}$ with the property that for all $\alpha \in \mathbb{L}$ and all $(s,t) \in R_\alpha$,

- whenever $s \overset{k}{\dashrightarrow}_S s'$, then there is $\beta \in \mathbb{L}$ and $(s',t') \in R_\beta$ for which $t \overset{\ell}{\dashrightarrow}_T t'$ and $F(k,\ell,\beta) \sqsubseteq_{\mathbb{L}} \alpha$,
- whenever $t \overset{\ell}{\longrightarrow}_T t'$, then there is $\beta \in \mathbb{L}$ and $(s',t') \in R_\beta$ for which $s \overset{k}{\longrightarrow}_S s'$ and $F(k,\ell,\beta) \sqsubseteq_{\mathbb{L}} \alpha$.

Additionally we assume R to be *closed* in the sense that for all $s \in S$, $t \in T$, $(s,t) \in R_{\inf\{\alpha \mid (s,t) \in R_\alpha\}}$.

Lemma 1. *For all SMTS S, T, $S \leq_m^\alpha T$ if and only if there is a modal refinement family R from S to T with $(s_0,t_0) \in R_\alpha$.*

We say that a modal refinement family as in the lemma *witnesses* $S \leq_m^\alpha T$.

Proof (of Lemma 1). Assume first that $S \leq_m^\alpha T$, thus we know that $d_m(S,T) \sqsubseteq_{\mathbb{L}} \alpha$. We have to show that there is a modal refinement family R from S to T with $(s_0,t_0) \in R_\alpha$. Define a family $R = \{R_\alpha \subseteq S \times T \mid \alpha \in \mathbb{L}\}$ by

$$R_\alpha = \{(s,t) \mid d_m(s,t) \sqsubseteq_{\mathbb{L}} \alpha\}$$

for every $\alpha \in \mathbb{L}$; note that R is closed in the sense above. Now let $\beta \in \mathbb{L}$ and $(s,t) \in R_\beta$.

- Assume $s \overset{k}{\dashrightarrow} s'$. By $d_m(s,t) \sqsubseteq_{\mathbb{L}} \beta$ and the definition of $d_m(s,t)$ it follows that $\inf_{t \overset{\ell}{\dashrightarrow} t'} F(k,\ell,d_m(s',t')) \sqsubseteq_{\mathbb{L}} \beta$. As T is compactly branching and F continuous, the set $\{F(k,\ell,d_m(s',t')) \mid t \overset{\ell}{\dashrightarrow} t'\}$ is compact, hence there exists a transition $t \overset{\ell}{\dashrightarrow} t'$ such that $F(k,\ell,d_m(s',t')) \sqsubseteq_{\mathbb{L}} \beta$.
- Assume $t \overset{\ell}{\longrightarrow} t'$. By $d_m(s,t) \sqsubseteq_{\mathbb{L}} \beta$ and the definition of $d_m(s,t)$ it follows that $\inf_{s \overset{k}{\longrightarrow} s'} F(k,\ell,d_m(s',t')) \sqsubseteq_{\mathbb{L}} \beta$. Again $\{F(k,\ell,d_m(s',t')) \mid s \overset{k}{\longrightarrow} s'\}$ is a compact set, whence there exists a transition $s \overset{k}{\longrightarrow} s'$ such that $F(k,\ell,d_m(s',t')) \sqsubseteq_{\mathbb{L}} \beta$.

For the other direction, assume a refinement family R from S to T with $(s_0,t_0) \in R_\alpha$. Define $h : S \times T \to \mathbb{L}$ by $h(s,t) = \inf\{\alpha \mid (s,t) \in R_\alpha\}$. Then $(s,t) \in R_\beta$ implies that $h(s,t) \sqsubseteq_{\mathbb{L}} \beta$. Let $s \in S$ and $t \in T$, then $(s,t) \in R_{h(s,t)}$ because R is closed, hence for all $s \overset{k}{\dashrightarrow} s'$ there is $t \overset{\ell}{\dashrightarrow} t'$ and $\alpha' \in \mathbb{L}$ for which $F(k,\ell,\alpha') \sqsubseteq_{\mathbb{L}} h(s,t)$ and $(s',t') \in R_{\alpha'}$, implying $h(s',t') \sqsubseteq_{\mathbb{L}} \alpha'$ and hence $F(k,\ell,h(s',t')) \sqsubseteq_{\mathbb{L}} h(s,t)$ by monotonicity and transitivity. Similarly, for all $t \overset{\ell}{\longrightarrow} t'$ there is $s \overset{k}{\longrightarrow} s'$ with $F(k,\ell,h(s',t')) \sqsubseteq_{\mathbb{L}} h(s,t)$. Hence h is a pre-fixed point for the equations in the definition of d_m, implying that $d_m(s,t) \sqsubseteq_{\mathbb{L}} h(s,t)$ for all $s \in S$, $t \in T$, thus especially $d_m(s_0,t_0) \sqsubseteq_{\mathbb{L}} \alpha$, because $(s_0,t_0) \in R_\alpha$ implies $h(s_0,t_0) \sqsubseteq_{\mathbb{L}} \alpha$ and $d_m(s_0,t_0) \sqsubseteq_{\mathbb{L}} h(s_0,t_0)$. □

Proof (of Theorem 1). If $d_m(S,T) = \top_{\mathbb{L}}$, we have nothing to prove. Otherwise, let $R = \{R_\alpha \subseteq S \times T \mid \alpha \in \mathbb{L}\}$ be a modal refinement family which witnesses $d_m(S,T)$, and let $I \in [\![S]\!]$. We will expose $J \in [\![T]\!]$ for which $d_m(I,J) \sqsubseteq_{\mathbb{L}} d_m(S,T)$.

Let $R^1 \subseteq I \times S$ be a witness for $I \leq_m S$, define $R'_\alpha = R^1 \circ R_\alpha \subseteq I \times T$ for all $\alpha \in \mathbb{L}$, and let $R' = \{R'_\alpha \mid \alpha \in \mathbb{L}\}$. We let the states of J be $J = T$, with $j_0 = t_0$, and define $\dashrightarrow_J = \longrightarrow_J$ as follows:

For any $i \xrightarrow{m}_I i'$ and any $t \in T$ for which $(i,t) \in R'_\alpha \in R'$ for some $\alpha \in \mathbb{L}$, $\alpha \neq \top_{\mathbb{L}}$, we have $t \overset{\ell}{\dashrightarrow}_T t'$ with $(i',t') \in R'_\beta \in R'$ for some $\beta \in \mathbb{L}$ with $F(m,\ell,\beta) \sqsubseteq_{\mathbb{L}} \alpha$. As $[\![\ell]\!]$ is closed under F, there is $n \in [\![\ell]\!]$ for which $F(m,n,\beta) = F(m,\ell,\beta)$, and we add a transition $t \xrightarrow{n}_J t'$ to J.

Similarly, for any $t \xrightarrow{\ell}_T t'$ and any $i \in I$ for which $(i,t) \in R'_\alpha \in R'$ for some $\alpha \in \mathbb{L}$, $\alpha \neq \top_{\mathbb{L}}$, we have $i \xrightarrow{m}_I i'$ with $(i',t') \in R'_\beta$ for some $\beta \in \mathbb{L}$ with $F(m,\ell,\beta) \sqsubseteq_{\mathbb{L}} \alpha$. Using again closedness of $[\![\ell]\!]$, we find $n \in [\![\ell]\!]$ for which $F(m,n,\beta) = F(m,\ell,\beta)$ and add a transition $t \xrightarrow{n}_J t'$ to J.

We show that the identity relation $\{(t,t) \mid t \in T\} \subseteq J \times T$ witnesses $J \leq_m T$. Let first $t \xrightarrow{n}_J t'$; we must have used one of the two constructions above for creating this transition. In the first case, there is $t \overset{\ell}{\dashrightarrow}_T t'$ with $n \in [\![\ell]\!]$, and in the second case, there is $t \xrightarrow{\ell}_T t'$, hence also $t \overset{\ell'}{\dashrightarrow}_T t'$ with $\ell \sqsubseteq_{\mathsf{Spec}} \ell'$, thus $n \in [\![\ell]\!] \subseteq [\![\ell']\!]$. Now let $t \xrightarrow{\ell}_T t'$, then the second construction above has introduced $t \xrightarrow{n}_J t'$ with $n \in [\![\ell]\!]$.

To finish the proof, we show that the family R' is a witness for $d_m(I,J) \sqsubseteq_{\mathbb{L}} d_m(S,T)$. First, $(i_0,s_0) \in R^1$ and $(s_0,t_0) \in R_{d_m(S,T)}$ imply $(i_0,t_0) \in R'_{d_m(S,T)}$. Let $(i,t) \in R'_\alpha \in R'$ for some $\alpha \in \mathbb{L}$, $\alpha \neq \top_{\mathbb{L}}$, and assume first $i \xrightarrow{m}_I i'$. Then $t \overset{\ell}{\dashrightarrow}_T t'$ and $t \xrightarrow{n}_J t'$ by the first part of our above construction, and $(i',t') \in R'_\beta$ with $F(m,n,\beta) \sqsubseteq_{\mathbb{L}} F(m,\ell,\beta) \sqsubseteq_{\mathbb{L}} \alpha$. For the converse, and transition $t \xrightarrow{n}_J t'$ must have been introduced above, and in both cases, $i \xrightarrow{m}_I i'$ with $(i',t') \in R'_\beta$ and $F(m,n,\beta) \sqsubseteq_{\mathbb{L}} F(m,\ell,\beta) \sqsubseteq_{\mathbb{L}} \alpha$. □

If $d_t(S,T) = \top_{\mathbb{L}}$, we are done. Otherwise we inductively construct a relation family $R = \{R_\alpha \subseteq S \times T \mid \alpha \in \mathbb{L}\}$ which satisfies $d_t((s,S),(t,T)) \sqsubseteq \alpha$ for any $(s,t) \in R_\alpha$, as follows: Begin by letting $R_\alpha = \{(s_0,t_0)\}$ for all $\alpha \sqsupseteq_{\mathbb{L}} d_t(S,T)$, and let now $(s,t) \in R_\alpha$ with $d_t((s,S),(t,T)) \sqsubseteq \alpha \neq \top_{\mathbb{L}}$.

Let $s \overset{k}{\dashrightarrow}_S s'$ and $t \overset{\ell}{\dashrightarrow}_T t'$ such that $d(k,\ell) \neq \top_{\mathbb{L}}$. Let $(i',I') \in [\![(s',S)]\!]$ and $m \in [\![k]\!]$, then there is $(i,I) \in [\![(s,S)]\!]$ for which $i \xrightarrow{m}_I i''$ and $(i'',I) \leq_m (i',I')$. By the triangle inequality we have $d_t((i,I),(t,T)) \sqsubseteq_{\mathbb{L}} d_t((i,I),(s,S)) \oplus_{\mathbb{L}} d_t((s,S),(t,T)) \sqsubseteq_{\mathbb{L}} \alpha$, hence there is $t \overset{\ell'}{\dashrightarrow} t''$ for which $d(m,\ell') \sqsubseteq_{\mathbb{L}} \alpha$. But we also have $d(m,\ell) \sqsubseteq_{\mathbb{L}} d(m,k) \oplus_{\mathbb{L}} d(k,\ell) = d(k,\ell) \neq \top_{\mathbb{L}}$, so by determinism of T it follows that $\ell = \ell'$ and $t' = t''$.

As $m \in [\![k]\!]$ was chosen arbitrarily above, we have $d(m,\ell) \sqsubseteq_{\mathbb{L}} \alpha$ for all $m \in [\![k]\!]$, hence $d(k,\ell) = F(k,\ell,\bot_{\mathbb{L}}) \sqsubseteq \alpha$. Let $B = \{\beta' \in \mathbb{L} \mid F(k,\ell,\beta') \sqsubseteq_{\mathbb{L}} \alpha\}$ and $\beta = \sup B$, then $F(k,\ell,\beta) \sqsubseteq_{\mathbb{L}} \alpha$ as $\bot_{\mathbb{L}} \in S$. Add (s',t') to R_γ for all $\gamma \sqsupseteq_{\mathbb{L}} \beta$.

We miss to show that $d_t((s',S),(t',T)) \sqsubseteq_{\mathbb{L}} \beta$. By $d_t((s,S),(t,T)) \sqsubseteq_{\mathbb{L}} \alpha$ we must have $(j,J) \in [\![(t,T)]\!]$, $j \xrightarrow{n}_J j'$, and $\beta' \in \mathbb{L}$ for which $d_m((i',I'),(j',J)) \sqsubseteq_{\mathbb{L}} \beta'$ and $F(m,n,\beta') \sqsubseteq_{\mathbb{L}} \alpha$. Then $F(k,\ell,\beta') = F(m,\ell,\beta') \sqsubseteq_{\mathbb{L}} F(m,n,\beta') \sqsubseteq_{\mathbb{L}} \alpha$, hence $\beta' \in B$, implying that $d_t((s',S),(t',T)) \sqsubseteq_{\mathbb{L}} \beta' \sqsubseteq_{\mathbb{L}} \beta$.

We show that R is a refinement family which witnesses $d_m(S,T)$. Let $(s,t) \in R_\alpha \in R$ for some $\alpha \in \mathbb{L}$ and assume $s \overset{k}{\dashrightarrow}_S s'$. Let $m \in [\![k]\!]$, then there is $(i,I) \in [\![(s,S)]\!]$ with $i \xrightarrow{m}_I i'$. As $d_t((i,I),(t,T)) \sqsubseteq_{\mathbb{L}} \alpha$, this implies that there is $t \overset{\ell}{\dashrightarrow}_T t'$ with $d(m,\ell) \sqsubseteq_{\mathbb{L}} \alpha$. Also for any other $m' \in [\![k]\!]$ we have $t \overset{\ell'}{\dashrightarrow}_T t''$ with $d(m,\ell') \sqsubseteq_{\mathbb{L}} \alpha$, hence $\ell = \ell'$ and $t' = t''$ by determinism. As m was chosen arbitrarily, we have $d(m,\ell) \sqsubseteq \alpha$ for all $m \in [\![k]\!]$, hence $d(k,\ell) = F(k,\ell,\bot_{\mathbb{L}}) \sqsubseteq \alpha$. By construction of R, $(s',t') \in R_\beta$ for $\beta = \sup\{\beta' \in \mathbb{L} \mid F(k,\ell,\beta') \sqsubseteq_{\mathbb{L}} \alpha\}$.

Now assume $t \xrightarrow{\ell}_T t'$. Let $(i,I) \in [\![(s,S)]\!]$, then we have $(j,J) \in [\![(t,T)]\!]$ with $d_m((i,I),(j,J)) \sqsubseteq_{\mathbb{L}} \alpha$. We must have $j \xrightarrow{n}_J j'$ with $n \in [\![\ell]\!]$, hence there are $i \xrightarrow{m}_I i'$ and $\beta' \in \mathbb{L}$ with $d_m((i',I),(j',J)) \sqsubseteq_{\mathbb{L}} \beta'$ and $F(m,n,\beta') \sqsubseteq_{\mathbb{L}} \alpha$.

The above considerations hold for all $(i,I) \in [\![(s,S)]\!]$, hence there is $k \in \mathbb{L}$ with $m \in [\![k]\!]$, $s \xrightarrow{k}_S s'$, and $F(k,\ell,\beta') = F(m,\ell,\beta')$. But then $F(k,\ell,\beta') \sqsubseteq_{\mathbb{L}} F(m,n,\beta') \sqsubseteq_{\mathbb{L}} \alpha$, hence by construction of R, $(s',t') \in R_\beta$ for $\beta = \sup\{\beta' \in \mathbb{L} \mid F(k,\ell,\beta') \sqsubseteq_{\mathbb{L}} \alpha\}$. □

Proof (of Proposition 3). An application of the triangle inequality for d_m:

$$
\begin{aligned}
&d_m(S,S') \sqsubseteq_{\mathbb{L}} d_m(S,T') \oplus_{\mathbb{L}} d_m(T',S') \sqsubseteq_{\mathbb{L}} d_m(S,T') \oplus_{\mathbb{L}} \alpha' \\
&d_m(S,T') \sqsubseteq_{\mathbb{L}} d_m(S,S') \oplus_{\mathbb{L}} d_m(S',T') = d_m(S,S') \\
&d_m(S,S') \sqsubseteq_{\mathbb{L}} d_m(S,T) \oplus_{\mathbb{L}} d_m(T,S') = d_m(T,S') \\
&d_m(T,S') \sqsubseteq_{\mathbb{L}} d_m(T,S) \oplus_{\mathbb{L}} d_m(S,S') \sqsubseteq \alpha \oplus_{\mathbb{L}} d_m(S,S')
\end{aligned}
$$

□

Proof (of Theorem 2). The proof of the first claim is in [2]. For the second claim, let $R = \{R_\alpha \subseteq S \times T \mid \alpha \in \mathbb{L}\}$, $R' = \{R'_\alpha \subseteq S' \times T' \mid \alpha \in \mathbb{L}\}$ be witnesses for $d_m(S,T)$ and $d_m(S',T')$, respectively, and define

$$
\begin{aligned}
R^{\|}_\beta = \{((s,s'),(t,t')) \in S \times S' \times T \times T' \mid \\
\exists \alpha,\alpha' \in \mathbb{L} : (s,t) \in R_\alpha \in R, (s',t') \in R'_{\alpha'} \in R', P(\alpha,\alpha') \sqsubseteq_{\mathbb{L}} \beta\}
\end{aligned}
$$

for all $\beta \in \mathbb{L}$. We show that $R^{\|} = \{R^{\|}_\beta \mid \beta \in L\}$ is a witness for $d_m(S\|S',T\|T') \sqsubseteq_{\mathbb{L}} P(d_m(S,T),d_m(S',T'))$.

First, $((s_0,s'_0),(t_0,t'_0)) \in R^{\|}_{P(d_m(S,T),d_m(S',T'))}$. Let now $\beta \in \mathbb{L} \setminus \{\top_{\mathbb{L}}\}$ and $((s,s'),(t,t')) \in R^{\|}_\beta \in R^{\|}$, then we have $\alpha,\alpha' \in \mathbb{L} \setminus \{\top_{\mathbb{L}}\}$ with $(s,t) \in R_\alpha \in R$, $(s',t') \in R'_{\alpha'} \in R'$, and $P(\alpha,\alpha') \sqsubseteq_{\mathbb{L}} \beta$.

Let $(s,s') \overset{k \mathbin{\mathbb{O}} k'}{\dashrightarrow}_{S\|S'} (\bar{s},\bar{s}')$, then $s \overset{k}{\dashrightarrow}_S \bar{s}$ and $s' \overset{k'}{\dashrightarrow}_{S'} \bar{s}'$. As $(s,t) \in R_\alpha \in R$, we have $t \overset{\ell}{\dashrightarrow}_T \bar{t}$ and $\bar{\alpha} \in \mathbb{L}$ with $(\bar{s},\bar{t}) \in R_{\bar{\alpha}} \in R$ and $F(k,\ell,\bar{\alpha}) \sqsubseteq_{\mathbb{L}} \alpha$. Similarly, $(s',t') \in R'_{\alpha'} \in R'$ implies that there is $t' \overset{\ell'}{\dashrightarrow}_{T'} \bar{t}'$ and $\bar{\alpha}' \in \mathbb{L}$ with $(\bar{s}',\bar{t}') \in R'_{\bar{\alpha}'} \in R'$ and $F(k',\ell',\bar{\alpha}') \sqsubseteq_{\mathbb{L}} \alpha'$.

As $F(k,\ell,\bar\alpha) \neq \top_{\mathbb{L}}$ and $F(k',\ell',\alpha') \neq \top_{\mathbb{L}}$, the composition $\ell \oplus \ell'$ is defined, and we have $(t,t') \overset{\ell\oplus\ell'}{\dashrightarrow}_{T\|T'} (\bar t,\bar t')$ by definition of $S\|S'$. Also, $(\bar t,\bar t') \in R^{\|}_{P(\bar\alpha,\bar\alpha')} \in R^{\|}$ and $F(k \oplus k', \ell\oplus\ell', P(\bar\alpha,\bar\alpha')) \sqsubseteq_{\mathbb{L}} P(F(k,\ell,\bar\alpha), F(k',\ell',\bar\alpha')) \sqsubseteq_{\mathbb{L}} P(\alpha,\alpha')$.

The reverse direction, assuming a transition $(t,t') \overset{\ell\oplus\ell'}{\longrightarrow}_{T\|T'} (\bar t,\bar t')$, is similar. □

Proof (of Theorem 3). The proof that $X \leq_m T \setminus\!\setminus S$ if and only if $S\|X \leq_m T$ is in [2]. For the other properties, assume first $\oslash$ to be quantitatively well-behaved; we show that $d_m(S\|X,T) \sqsubseteq_{\mathbb{L}} d_m(X, T \setminus\!\setminus S)$. If $d_m(X,T\setminus\!\setminus S) = \top_{\mathbb{L}}$, there is nothing to prove, so assume $d_m(X,T\setminus\!\setminus S) \neq \top_{\mathbb{L}}$ and let $R = \{R_\alpha \subseteq X \times (T \times S \cup \{u\})\}$ be a witness for $d_m(X,T\setminus\!\setminus S)$. Define $R'_\alpha = \{((s,x),t) \mid (x,(t,s)) \in R_\alpha\} \subseteq S \times X \times T$ for all $\alpha \in \mathbb{L}$ and collect these to a family $R' = \{R'_\alpha \mid \alpha \in \mathbb{L}\}$. We show that R' is a witness for $d_m(S\|X,T) \sqsubseteq_{\mathbb{L}} d_m(X, T\setminus\!\setminus S)$.

We have $((s_0,x_0),t_0) \in R'_{d_m(X,T\setminus\!\setminus S)} \in R'$, so let $\alpha \in \mathbb{L}$ and $((s,x),t) \in R'_\alpha \in R'$, and assume first that $(s,x) \overset{k\oplus m}{\dashrightarrow}_{S\|X} (s',x')$. Then $s \overset{k}{\dashrightarrow}_S s'$ and $x \overset{m}{\dashrightarrow}_X x'$ by definition of $S\|X$. Now $(x,(t,s)) \in R_\alpha \in R$ implies that there is $(t,s) \overset{\ell\oslash k'}{\dashrightarrow}_{T\setminus\!\setminus S} (t',s'')$ and $\alpha' \in \mathbb{L}$ for which $F(m,\ell\oslash k',\alpha') \sqsubseteq_{\mathbb{L}} \alpha$ and $(x',(t',s'')) \in R_{\alpha'} \in R$. But then also $((s'',x'),t') \in R'_\alpha \in R'$, hence $k' \oplus m$ is defined and $F(k'\oplus m,\ell,\alpha') \sqsubseteq_{\mathbb{L}} F(m,\ell\oslash k',\alpha') \sqsubseteq_{\mathbb{L}} \alpha$.

Now $k \oplus m$ and $k' \oplus m$ being defined implies that there is k'' for which $d(k'',k) \neq \top_{\mathbb{L}}$ and $d(k'',k') \neq \top_{\mathbb{L}}$, and by definition of $T \setminus\!\setminus S$, $s \overset{k'}{\dashrightarrow}_S s''$. As S is deterministic, this implies $k = k'$ and $s' = s''$. Hence $((s',x'),t') \in R'_{\alpha'} \in R'$ and $F(k\oplus m,\ell,\alpha') \sqsubseteq_{\mathbb{L}} \alpha$.

Assume now that $t \overset{\ell}{\longrightarrow}_T t'$. We must have $s \overset{k}{\longrightarrow}_S s'$ for which $\ell \oslash k$ is defined, for otherwise $(t,s) \in B$ and hence (t,s) would have been pruned in $T\setminus\!\setminus S$. Thus $(t,s) \overset{\ell\oslash k}{\longrightarrow}_{T\setminus\!\setminus S} (t',s')$, which by $(x,(t,s)) \in R_\alpha \in R$ implies that there is $x \overset{m}{\longrightarrow}_X x'$ and $\alpha' \in \mathbb{L}$ for which $F(m,\ell\oslash k,\alpha') \sqsubseteq_{\mathbb{L}} \alpha$ and $(x',(t',s')) \in R_{\alpha'} \in R$, hence $((s',x'),t') \in R'_{\alpha'} \in R'$. But then $k \oplus m$ is defined and $F(k\oplus m,\ell,\alpha') \sqsubseteq_{\mathbb{L}} F(m,\ell\oslash k,\alpha') \sqsubseteq_{\mathbb{L}} \alpha$, and $(s,x) \overset{k\oplus m}{\longrightarrow}_{S\|X} (s',x')$.

Let now $\oslash$ be quantitatively exact. To show that $d_m(X,T\setminus\!\setminus S) \sqsubseteq_{\mathbb{L}} d_m(S\|X,T)$, assume that $d_m(S\|X,T) \neq \top_{\mathbb{L}}$ (otherwise there is nothing to prove), let $R = \{R_\alpha \subseteq S \times X \times T \mid \alpha \in \mathbb{L}\}$ be a witness for $d_m(S\|X,T)$, and define $R'_\alpha = \{(x,(t,s)) \mid ((s,x),t) \in R_\alpha\} \cup \{(x,u) \mid x \in X\} \subseteq X \times (T \times S \cup \{u\})$ for all $\alpha \in \mathbb{L}$. We show that $R' = \{R'_\alpha \mid \alpha \in \mathbb{L}\}$ is a witness for $d_m(X,T\setminus\!\setminus S) \sqsubseteq_{\mathbb{L}} d_m(S\|X,T)$.

We have $(x_0,(t_0,s_0)) \in R'_{d_m(S\|X,T)} \in R'$. Let $\alpha \in \mathbb{L}$, $(x,u) \in R'_\alpha \in R'$ and $x \overset{m}{\dashrightarrow}_X x'$, then also $u \overset{m}{\dashrightarrow}_{T\setminus\!\setminus S} u$, $F(m,m,\bot_{\mathbb{L}}) \sqsubseteq \alpha$, and $(x',u) \in R'_{\bot_{\mathbb{L}}} \in R'$. Now let $(x,(t,s)) \in R'_\alpha \in R'$ and $x \overset{m}{\dashrightarrow}_X x'$. If $k \oplus m$ is undefined for all $s \overset{k}{\dashrightarrow}_S s'$, then by definition of $T \setminus\!\setminus S$, $(t,s) \overset{m}{\dashrightarrow}_{T\setminus\!\setminus S} u$, $F(m,m,\bot_{\mathbb{L}}) \sqsubseteq \alpha$, and $(x',u) \in R'_{\bot_{\mathbb{L}}} \in R'$.

If there is a transition $s \overset{k}{\dashrightarrow}_S s'$ for which $k \oplus m$ is defined (by determinism there can be at most one), then also $(s,x) \overset{k\oplus m}{\dashrightarrow}_{S\|X} (s',x')$. As $((s,x),t) \in$

$R_\alpha \in R$, we must have $t \overset{\ell}{\dashrightarrow} t'$ and $\alpha' \in \mathbb{L}$ with $F(k \oplus m, \ell, \alpha') \sqsubseteq_{\mathbb{L}} \alpha$ and $((s', x'), t') \in R_{\alpha'} \in R$, hence $(x', (t', s')) \in R'_{\alpha'} \in R'$. Then $\ell \oslash k$ is defined and $F(m, \ell \oslash k, \alpha') \sqsubseteq_{\mathbb{L}} \alpha$, and by definition of $T \setminus\!\setminus S$, $(t, s) \overset{\ell \oslash k}{\dashrightarrow}_{T \setminus\!\setminus S} (t', s')$.

Now assume that $(t, s) \overset{\ell \oslash k}{\longrightarrow}_{T \setminus\!\setminus S} (t', s')$, then $t \overset{\ell}{\longrightarrow}_T t'$ and $s \overset{k}{\longrightarrow}_S s'$ by definition of $T \setminus\!\setminus S$. By $((s, x), t) \in R_\alpha \in R$, we have $(s, x) \overset{k' \oplus m}{\longrightarrow}_{S \| X} (s'', x')$ and $\alpha' \in \mathbb{L}$ with $F(k' \oplus m, \ell, \alpha') \sqsubseteq_{\mathbb{L}} \alpha$ and $((s'', x'), t') \in R_{\alpha'} \in R$. This in turn implies that $s \overset{k'}{\longrightarrow}_S s''$ and $x \overset{m}{\longrightarrow}_X s'$ by definition of $S \| X$. We also see that $\ell \oslash k'$ is defined, which by determinism of S entails $k = k'$ and $s' = s''$. Hence $F(k \oplus m, \ell, \alpha') \sqsubseteq_{\mathbb{L}} \alpha$ and $(x', (t', s')) \in R'_{\alpha'} \in R'$. □

Proof (of Theorem 4). The proof of the two first claims is in [2]. For the third claim, let $R = \{R_\alpha \subseteq U \times S \mid \alpha \in \mathbb{L}\}$ and $R' = \{R'_\alpha \subseteq U \times T \mid \alpha \in \mathbb{L}\}$ be relation families witnessing $d_m(U, S)$ and $d_m(U, T)$, respectively, define $R^\wedge_\beta = \{(u, (s, t)) \mid \exists \alpha, \alpha' \in \mathbb{L} : (u, s) \in R_\alpha, (u, t) \in R'_{\alpha'}, C(\alpha, \alpha') \sqsubseteq_{\mathbb{L}} \beta\} \subseteq U \times S \times T$ for all $\beta \in \mathbb{L}$, and let $R^\wedge = \{R^\wedge_\beta \mid \beta \in \mathbb{L}\}$. We show that $R^\wedge$ is a witness for $d_m(U, S \wedge T) \sqsubseteq_{\mathbb{L}} C(d_m(U, S), d_m(U, T))$.

We have $(u_0, (s_0, t_0)) \in R^\wedge_{C(d_m(U,S), d_m(U,T))} \in R^\wedge$. Let $\beta \in \mathbb{L} \setminus \{\bot_{\mathbb{L}}\}$ and $(u, (s, t)) \in R^\wedge_\beta \in R^\wedge$, then we have $\alpha, \alpha' \in \mathbb{L} \setminus \{\bot_{\mathbb{L}}\}$ with $(u, s) \in R_\alpha \in R$, $(u, t) \in R'_{\alpha'} \in R'$, and $C(\alpha, \alpha') \sqsubseteq_{\mathbb{L}} \beta$.

Assume $u \overset{m}{\dashrightarrow}_U u'$, then there exist $s \overset{k}{\dashrightarrow}_S s'$ and $\bar\alpha \in \mathbb{L}$ for which $(u', s') \in R_{\bar\alpha} \in R$ and $F(m, k, \bar\alpha) \sqsubseteq_{\mathbb{L}} \alpha$, and similarly $t \overset{\ell}{\dashrightarrow}_T t'$ and $\bar\alpha'$ with $(u', t') \in R'_{\bar\alpha'} \in R'$ and $F(m, \ell, \bar\alpha') \sqsubseteq \alpha'$. Then $d(m, k) \neq \top_{\mathbb{L}}$ and $d(m, \ell) \neq \top_{\mathbb{L}}$, so by conjunctive boundedness $k \oslash \ell$ is defined, and $(s, t) \overset{k \oslash \ell}{\dashrightarrow}_{S \wedge T} (s', t')$ by definition of $S \wedge T$. Also, $(u', (s', t')) \in R^\wedge_{C(\bar\alpha, \bar\alpha')} \in R^\wedge$ and $F(m, k \oslash \ell, C(\bar\alpha, \bar\alpha')) \sqsubseteq_{\mathbb{L}} C(F(m, k, \bar\alpha), F(m, \ell, \bar\alpha')) \sqsubseteq_{\mathbb{L}} C(\alpha, \alpha')$.

Assume $(s, t) \overset{k \oslash \ell}{\longrightarrow}_{S \wedge T} (s', t')$, then $s \overset{k}{\longrightarrow}_S s'$ and $t \overset{\ell}{\longrightarrow}_T t'$ by definition of $S \wedge T$. We can without loss of generality postulate that T is deterministic. The fact that $(u, s) \in R_\alpha \in R$ implies that there are $u \overset{m}{\longrightarrow}_U u'$ and $\bar\alpha \in \mathbb{L}$ for which $(u', s') \in R_{\bar\alpha} \in R$ and $F(m, k, \bar\alpha) \sqsubseteq_{\mathbb{L}} \alpha$. We must also have $u \overset{m'}{\dashrightarrow}_U u'$ for some $m' \sqsupseteq_{\mathsf{Spec}} m$, and then $(u, t) \in R'_{\bar\alpha} \in R'$ implies that there exist $t \overset{\ell'}{\dashrightarrow}_T t''$ and $\bar\alpha' \in \mathbb{L}$ with $(u', t'') \in R'_{\bar\alpha'} \in R'$ and $F(m', \ell', \bar\alpha') \sqsubseteq_{\mathbb{L}} \alpha'$.

The triangle inequality for F gives $F(m, \ell', \bar\alpha') \sqsubseteq_{\mathbb{L}} F(m, m', \bot_{\mathbb{L}}) \oplus F(m', \ell', \bar\alpha') \sqsubseteq_{\mathbb{L}} \alpha'$, hence $d(m, \ell') \neq \top_{\mathbb{L}}$. Together with $d(m, k) \neq \top_{\mathbb{L}}$, conjunctive boundedness allows us to conclude that $k \oslash \ell'$ is defined, but then both $k \oslash \ell$ and $k \oslash \ell'$ are defined, hence by determinism of T, $\ell = \ell'$ and $t' = t''$. □

Proof (of Theorem 5). We start by constructing S' and T', almost as in the proof of the third claim of Theorem 4. The states of S' and T' will be the same as for S and T, and we start by letting $\beta = \bot_{\mathbb{L}}$, $\gamma = \bot_{\mathbb{L}}$.

Let U fulfill $d_m(U, S) \neq \top_{\mathbb{L}}$ and $d_m(U, T) \neq \top_{\mathbb{L}}$, let $R = \{R_\alpha \subseteq U \times S \mid \alpha \in \mathbb{L}\}$ and $R' = \{R'_\alpha \subseteq U \times T \mid \alpha \in \mathbb{L}\}$ be relation families witnessing $d_m(U, S)$ and $d_m(U, T)$, respectively, define $R^\wedge_\eta = \{(u, (s, t)) \mid \exists \alpha, \alpha' \in \mathbb{L} :$

$(u,s) \in R_\alpha, (u,t) \in R'_{\alpha'}, C(\alpha,\alpha',\bot_\mathbb{L},\bot_\mathbb{L}) \sqsubseteq_\mathbb{L} \eta\} \subseteq U \times S \times T$ for all $\eta \in \mathbb{L}$, and let $R^\wedge = \{R^\wedge_\eta \mid \eta \in \mathbb{L}\}$.

Now let $\eta \in \mathbb{L}\backslash\{\top_\mathbb{L}\}$ and $(u,(s,t)) \in R^\wedge_\eta \in R^\wedge$, then we have $\alpha,\alpha' \in \mathbb{L}\backslash\{\bot_\mathbb{L}\}$ with $(u,s) \in R_\alpha \in R$, $(u,t) \in R'_{\alpha'} \in R'$, and $C(\alpha,\alpha',\bot_\mathbb{L},\bot_\mathbb{L}) \sqsubseteq_\mathbb{L} \eta$. Let $u \overset{m}{\dashrightarrow}_U u'$, then also $s \overset{k}{\dashrightarrow}_S s'$ and $t \overset{\ell}{\dashrightarrow}_T t'$, and there are $\bar\alpha,\bar\alpha' \in \mathbb{L} \setminus \{\top_\mathbb{L}\}$ with $F(m,k,\bar\alpha) \sqsubseteq_\mathbb{L} \alpha$ and $F(m,\ell,\bar\alpha') \sqsubseteq_\mathbb{L} \alpha'$. Hence $d(m,k) \neq \top_\mathbb{L}$ and $d(m,\ell) \neq \top_\mathbb{L}$, and by relaxed conjunctive boundedness we have $k',\ell' \in \mathsf{Spec}$ with $k \sqsubseteq_\mathsf{Spec} k'$, $\ell \sqsubseteq_\mathsf{Spec} \ell'$, $d(k',k) \neq \top_\mathbb{L}$, $d(\ell',\ell) \neq \top_\mathbb{L}$, and $k' \wedge \ell'$ defined. We add the transitions $s \overset{k'}{\dashrightarrow}_{S'} s'$, $t \overset{\ell'}{\dashrightarrow}_{T'} t'$ to S' and T' and update $\beta := \max(\beta, d(k',k))$, $\gamma := \max(\gamma, d(\ell',\ell))$.

As the sets $\{k \in \mathsf{Spec} \mid s \overset{k}{\dashrightarrow}_S s'\}$, $\{\ell \in \mathsf{Spec} \mid t \overset{\ell}{\dashrightarrow}_T t'\}$ are compact, the above process converges to some $\beta,\gamma \neq \top_\mathbb{L}$. The *must* transitions we just copy from S to S' and from T to T', and then S' is a β-widening of S and T' is a γ-widening of T.

We must show that S' and T' satisfy the properties claimed. By construction $S' \wedge T'$ is defined, so let U be an SMTS with $d_m(U,S) \neq \top_\mathbb{L}$ and $d_m(U,T) \neq \top_\mathbb{L}$. We must show that $d_m(U,S' \wedge T') \sqsubseteq_\mathbb{L} C_{\beta,\gamma}(d_m(U,S), d_m(U,T))$. Let $R = \{R_\alpha \subseteq U \times S \mid \alpha \in \mathbb{L}\}$ and $R' = \{R'_\alpha \subseteq U \times T \mid \alpha \in \mathbb{L}\}$ be relation families witnessing $d_m(U,S)$ and $d_m(U,T)$, respectively, define $R^{\wedge'}_\eta = \{(u,(s,t)) \mid \exists \alpha,\alpha' \in \mathbb{L} : (u,s) \in R_\alpha, (u,t) \in R'_{\alpha'}, C_{\beta,\gamma}(\alpha,\alpha') \sqsubseteq_\mathbb{L} \eta\} \subseteq U \times S' \times T'$ for all $\eta \in \mathbb{L}$, and let $R^{\wedge'} = \{R^{\wedge'}_\eta \mid \eta \in \mathbb{L}\}$.

We have $(u_0,(s_0,t_0)) \in R^{\wedge'}_{C_{\beta,\gamma}(d_m(U,S),d_m(U,T))} \in R^{\wedge'}$. Let $\eta \in \mathbb{L} \setminus \{\bot_\mathbb{L}\}$ and $(u,(s,t)) \in R^{\wedge'}_\eta$, then we have $\alpha,\alpha' \in \mathbb{L} \setminus \{\bot_\mathbb{L}\}$ with $(u,s) \in R_\alpha \in R$, $(u,t) \in R'_{\alpha'} \in R'$, and $C_{\beta,\gamma}(\alpha,\alpha') \sqsubseteq_\mathbb{L} \eta$. Let $u \overset{m}{\dashrightarrow}_U u'$, then also $s \overset{k}{\dashrightarrow}_S s'$ and $t \overset{\ell}{\dashrightarrow}_T t'$, and there are $\bar\alpha,\bar\alpha' \in \mathbb{L} \setminus \{\top_\mathbb{L}\}$ with $(u',s') \in R_{\bar\alpha}$, $(u',t') \in R'_{\bar\alpha'}$, $F(m,k,\bar\alpha) \sqsubseteq_\mathbb{L} \alpha$, and $F(m,\ell,\bar\alpha') \sqsubseteq_\mathbb{L} \alpha'$.

By construction of S' and T', we have $s \overset{k'}{\dashrightarrow}_{S'} s'$ and $t \overset{\ell'}{\dashrightarrow}_{T'} t'$ with $k \sqsubseteq_\mathsf{Spec} k'$, $\ell \sqsubseteq_\mathsf{Spec} \ell'$, $d(k',k) \sqsubseteq_\mathbb{L} \beta$, and $d(\ell',\ell) \sqsubseteq_\mathbb{L} \gamma$, and such that $k' \oslash \ell'$ is defined. Also, $(u',(s',t')) \in R^{\wedge'}_{C_{\beta,\gamma}(\bar\alpha,\bar\alpha')}$ and $F(m,k' \oslash \ell', C_{\beta,\gamma}(\bar\alpha,\bar\alpha')) \sqsubseteq_\mathbb{L} C_{\beta,\gamma}(F(m,k,\bar\alpha), F(m,\ell,\bar\alpha')) \sqsubseteq_\mathbb{L} C_{\beta,\gamma}(\alpha,\alpha')$.

The other direction of the proof, starting with a transition $(s,t) \xrightarrow{k \oslash \ell}_{S' \wedge T'} (s',t')$, is an exact copy of the corresponding part of the proof of Theorem 4. □